```
############################################################
###

  Elliptic Curve Digital Signature Algorithm
     Curve: K-571
     Hash Algorithm: SHA-512

     Message to be signed: "Example of ECDSA with K-571"

############################################################
###

  Signature Generation
    H:
46E30ABDD459269CF19AF76900AF7131B4F639227414719EBEBE548CCD4
026B75C1F52618547AA3821F29FCF685E33640BD9E29F7FE46817627D41
39EEE411C6

    E:
46E30ABDD459269CF19AF76900AF7131B4F639227414719EBEBE548CCD4
026B75C1F52618547AA3821F29FCF685E33640BD9E29F7FE46817627D41
39EEE411C6

    K:
104063C918DE62000A3FD87775D8D71398722BD153B8EA33060349C5FE6
CF6CB4677957E6BA50D3C8A8B5182B9CF962954A6BBB5F7868B88E5778A
A62A0CF8002BF19DA3049FF51

    Kinv:
75A02BEAEA51660A1D05053B173C9C6DCCAEBA80F72CA08DEC3C32E2A47
CBC5674998AD19FC77B6615BFBED482451AF7FD9B416B64B0E8F8429449
FA9685F2B9C8DC2108544D98

    R_x:
668758C313FBF1945F775D95B25866DBC8D001D9C7EF4FFA53774E8C689
27A52707F034CEBB3A712BE6D164F2FFE1897B069F8FBAEC4650B5372DD
FA31CDECCFA78569197CF50F1

    R_y:
3796EAB7DA927707DF47EBED5898B37B053998C717BB726EBF552027255
B1222D0B088EFC8C03F9D855C8BF9ED19AECEA681C33CBBE5F539B3EF92
E98F88B2E75C1C7FB6D39F302

    R:
```

```
68758C313FBF1945F775D95B25866DBC8D001D9C7EF4FFA53774E8C6892
7A52707F034957247CB5717A5B6D84AE6F6C688DBE59859BD6D03B48237
476742AFE37CEFE36D5B20EE

    D:
1042FDE4D66E76725E7957E208A85CF23BC0D5B8D001B36AEAFB34AD110
4004CCF99AFDFABCA11585A4EB5263C87052CB05EF7FB39D9E5F6CF495E
9DCE5840B83FBC5FF3AD8B2F3

    S:
F5C8E975A1DA26B2E0ACD4F486C4A4231C1E29EE8ECFA03A697761498F5
D53FF898AFC16945975D328D34A8DCDC6D0613C73FE4F516F5685E23716
FE105ED3472C3358B5B4AD41

    Signature
        R:
68758C313FBF1945F775D95B25866DBC8D001D9C7EF4FFA53774E8C6892
7A52707F034957247CB5717A5B6D84AE6F6C688DBE59859BD6D03B48237
476742AFE37CEFE36D5B20EE

        S:
F5C8E975A1DA26B2E0ACD4F486C4A4231C1E29EE8ECFA03A697761498F5
D53FF898AFC16945975D328D34A8DCDC6D0613C73FE4F516F5685E23716
FE105ED3472C3358B5B4AD41

===========================================================
==

  Signature Verification
    Q_x:
<4D9CFE0A7338FEA703E007F5D10BABD2DF3F319B47DF1E23C4F7E5ABF5
014C1390B78F117E6AF8258A48F56ACB9FAAC788530B5CCDB1AB7E9390E
C5DD7A39D5EEAF6C41BF50AC76>
    Q_y:
<64732C504F81DC5F9B0E882B6DA46E124E8241358F077896D25ECF028A
D0E6011993C85E68741A07D7817C400CF94B1A3F524F48668B5B9709726
18616DB4362A769D16CAC34BF0>

    H:
<46E30ABDD459269CF19AF76900AF7131B4F639227414719EBEBE548CCD
4026B75C1F52618547AA3821F29FCF685E33640BD9E29F7FE46817627D4
139EEE411C6>

    E:
```

```
<46E30ABDD459269CF19AF76900AF7131B4F639227414719EBEBE548CCD
4026B75C1F52618547AA3821F29FCF685E33640BD9E29F7FE46817627D4
139EEE411C6>

    Sinv:
<7951DA1FAFEB8FF17C985C4C70715410F735637335988AD6F259609ABA
E17FD092C4E70FBEDFA531E157B9D532EE5F8AE97F0C8A6B70B4878D534
1AA7FBF55855B35EE72E1482F>

    U:
<121B1F8919C4ED41D4676BC6F417DBF7F93C2314C74796642D1B17DF4F
D04C114AE293707913E2EBB65E173D52C3678C8366EB3C94E7B7ECEE53F
6B0B625AC62B924E3D6B975FF3>

    V:
<1AFBF8D1D31511413EB6846B32CED90D38E515FF26CB8334EF61967779
4CC3B92DA014E9B0E39BF49D8933D3E998145594128612AECCBFC7004D0
8777FD90BC197D13DC6238BF0B>

    Rprime.X:
<668758C313FBF1945F775D95B25866DBC8D001D9C7EF4FFA53774E8C68
927A52707F034CEBB3A712BE6D164F2FFE1897B069F8FBAEC4650B5372D
DFA31CDECCFA78569197CF50F1>

    Rprime.Y:
<3796EAB7DA927707DF47EBED5898B37B053998C717BB726EBF55202725
5B1222D0B088EFC8C03F9D855C8BF9ED19AECEA681C33CBBE5F539B3EF9
2E98F88B2E75C1C7FB6D39F302>

    Rprime:
<68758C313FBF1945F775D95B25866DBC8D001D9C7EF4FFA53774E8C689
27A52707F034957247CB5717A5B6D84AE6F6C688DBE59859BD6D03B4823
7476742AFE37CEFE36D5B20EE>

Verification Passed!
```